ELSEVIER

Available online at www.sciencedirect.com
ScienceDirect

Discrete Mathematics 308 (2008) 631–644

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

# A general approach to constructing power-sequence terraces for $\mathbb{Z}_n$

Ian Anderson[a,*], D.A. Preece[b,c]

[a] *Department of Mathematics, University of Glasgow, University Gardens, Glasgow G12 8QW, UK*
[b] *School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK*
[c] *Institute of Mathematics, Statistics and Actuarial Science, Cornwallis Building, University of Kent, Canterbury, Kent CT2 7NF, UK*

Received 12 July 2005; accepted 11 July 2007
Available online 28 August 2007

**Abstract**

A terrace for $\mathbb{Z}_n$ is an arrangement $(a_1, a_2, \ldots, a_n)$ of the $n$ elements of $\mathbb{Z}_n$ such that the sets of differences $a_{i+1} - a_i$ and $a_i - a_{i+1}$ $(i = 1, 2, \ldots, n-1)$ between them contain each element of $\mathbb{Z}_n \backslash \{0\}$ exactly twice. For $n$ odd, many procedures have been published for constructing power-sequence terraces for $\mathbb{Z}_n$; each such terrace may be partitioned into segments one of which contains merely the zero element of $\mathbb{Z}_n$ whereas each other segment is either (a) a sequence of successive powers of an element of $\mathbb{Z}_n$ or (b) such a sequence multiplied throughout by a constant. We now present a new general power-sequence approach that yields $\mathbb{Z}_n$ terraces for all odd primes $n$ less than 1000 except for $n = 601$. It also yields terraces for some groups $\mathbb{Z}_n$ with $n = p^2$ where $p$ is an odd prime, and for some $\mathbb{Z}_n$ with $n = pq$ where $p$ and $q$ are distinct primes greater than 3. Each new terrace has at least one segment consisting of successive powers of 2, modulo $n$.


*MSC:* Primary 10A07; Secondary 05B30

*Keywords:* 2-sequencings; Half-and-half terraces; Power-sequence terraces; Primitive roots; Wieferich primes

## 1. Introduction

### 1.1. Basic definitions and notation

Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ be an arrangement of the elements of $\mathbb{Z}_n$, and let the ordered sequence $\mathbf{b} = (b_1, b_2, \ldots, b_{n-1})$ be defined by $b_i = a_{i+1} - a_i$ for $i = 1, 2, \ldots, n-1$. The arrangement $\mathbf{a}$ is a *terrace* for $\mathbb{Z}_n$, with $\mathbf{b}$ as the corresponding 2-*sequencing* or *quasi-sequencing* for $\mathbb{Z}_n$, if the sequences $\mathbf{b}$ and $-\mathbf{b}$ between them contain exactly two occurrences of each element $x$ from $\mathbb{Z}_n \backslash \{0\}$. Some expositions include the zero element of $\mathbb{Z}_n$ in $\mathbf{b}$, as an extra element at the start, but we find this practice inconvenient and we follow many a precedent by not adopting it. For convenience we may write "$\mathbb{Z}_n$ terrace" in place of "terrace for $\mathbb{Z}_n$".

Terraces were originally defined by Bailey [7] for a general finite group $G$, but the general case does not concern us here. Terraces are used in the construction of combinatorial designs used in statistical applications involving carry-over effects [7,1] and neighbour effects, but applications are not considered in the present paper.

* Corresponding author.
*E-mail address:* ia@maths.gla.ac.uk (I. Anderson).

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.07.051

For $n$ odd, a $\mathbb{Z}_n$ terrace is

- *half-and-half* [1, p. 42] if, for each element $x$ of $\mathbb{Z}_n\backslash\{0\}$, the set $\{b_1, b_2, \ldots, b_{(n-1)/2}\}$ contains either $+x$ or $-x$ exactly once;
- *narcissistic* [2, p. 32] if it is half-and-half and its 2-sequencing has $b_i = b_{n-i}$ for all $i = 1, 2, \ldots, (n-1)/2$;
- *segregated* [2, p. 33] if its middle element is 0 and its first $(n-1)/2$ elements are either all the squares of $\mathbb{Z}_n$ or all the non-squares of $\mathbb{Z}_n$.

Anderson and Preece [2–5] gave a wide selection of constructions for "power-sequence" terraces for $\mathbb{Z}_n$ where $n$ is odd. Each of these terraces can be partitioned into segments one of which contains merely the zero element of $\mathbb{Z}_n$, whereas each other segment is either (a) a sequence of successive powers of an element of $\mathbb{Z}_n$, or (b) such a sequence multiplied throughout by a constant. Many of the sequences $x^0, x^1, \ldots, x^{s-1}$ of distinct elements are "full-cycle" sequences such that $x^s = x^0$, but partial cycles are used too. As in previous papers, we use a fence (vertical bar) to separate two segments in a terrace, and use *fence difference* to denote the difference between the two elements on either side of a fence.

Although most of the constructions in the papers [2–5] are general, in the sense of producing infinite (or presumably infinite) series of terraces, they are mostly "special cases". By contrast, we now present a general constructional approach that is very powerful for odd primes $n$. This approach also yields terraces for some groups $\mathbb{Z}_n$ with $n = p^2$ where $p$ is an odd prime and for some $\mathbb{Z}_n$ with $n = pq$ where $p$ and $q$ are distinct primes greater than 3.

For $n$ odd, our new approach has two features. When the approach is applied to produce terraces with full-cycle segments only, these features are as follows:

- The terrace for $\mathbb{Z}_n$ includes the full-cycle segment
$$2^{-1}2^{-2}\ldots 2^1 2^0;$$
- Each other segment for units of $\mathbb{Z}_n$ is a full-cycle segment of the form
$$2^i\gamma\ \ 2^{2i}\gamma\ \ \ldots\ \ 2^{-i}\gamma\ \ 2^0\gamma,$$

where $\gamma \notin \langle 2\rangle$ and $2^i - 1 \in \langle 2\rangle$; here, as elsewhere, $\langle 2\rangle$ denotes the set of elements generated by 2.

If $-1 \in \langle 2\rangle$, then $2^f \equiv 2^{-f} \equiv -1 \pmod n$ where $\mathrm{ord}_n(2) = 2f$, so that $-2^i \equiv 2^{-(f-i)}$, and the full-cycle segments just given may perhaps be replaced by half-cycle segments of the forms

$$:+2^{-1}+2^{-2}\ldots-2^1-2^0:$$

and

$$:+2^i\gamma+2^{2i}\gamma\ldots-2^{-i}\gamma-2^0\gamma:,$$

where the colons at the start and end of a segment are a reminder that the segment contains only a half cycle.

For some classes of values of $n$, the merits of our approach are clearly established within the range $2 < n < 500$; we then restrict our tabulations of results to that range. For other classes of values of $n$, a clear picture must be obtained from the wider range $2 < n < 1000$.

At the risk of seeming illogical in our choice of notation, we find that clarity requires us to use bold *capitals* such as **A**, **P**, for certain sequences within terraces. We use $\mathbf{A}^{\mathrm{rev}}$ to denote the reverse of **A**, and so on.

### 1.2. Some number theory

For an understanding of the scope of theorems in Sections 3 and 4 below, we now present some simple results from number theory. These results are not commonly seen in quite the form that we need.

First we give some results for a general odd prime $p$ and its square $n = p^2$. We write $\mathbb{U}_p$ for the set of units of $\mathbb{Z}_p$, and $\mathbb{U}_n$ for the set of units of $\mathbb{Z}_n$. Thus $\mathbb{U}_p = \mathbb{Z}_p\backslash\{0\}$ and $\mathbb{U}_n = \mathbb{Z}_n\backslash p\mathbb{Z}_p$. We write $\langle 2\rangle_p$ for the subset of $\mathbb{U}_p$ that is generated by 2, modulo $p$, and $\langle 2\rangle_n$ for the subset of $\mathbb{U}_n$ that is generated by 2, modulo $n$. (We use obvious generalisations of this notation later in the paper.)

**Lemma 1.1.** *Let $p$ be an odd prime, and let $y$ be an element from $\mathbb{U}_p$. If $y^d \equiv 1 \pmod p$ for some integer $d$, then $y^{pd} \equiv 1 \pmod{p^2}$.*

**Proof.** We have $y^d = 1 + \lambda p$ for some integer $\lambda$, so $y^{pd} = (1 + \lambda p)^p = 1 + p\lambda p + \cdots \equiv 1 \pmod{p^2}$. □

**Theorem 1.1.** *Let $n = p^2$ where $p$ is an odd prime, and let $y$ be an element from $\mathbb{U}_p$. If $\mathrm{ord}_p(y) = d$, then $\mathrm{ord}_n(y) = d$ or $dp$.*

**Proof.** Suppose that $\mathrm{ord}_p(y) = d$ and $\mathrm{ord}_n(y) = D$. As $y^D \equiv 1 \pmod n$, we have $y^D \equiv 1 \pmod p$, so $d|D$. But $y^d \equiv 1 \pmod p$ so, by Lemma 1.1, we have $y^{pd} \equiv 1 \pmod n$, whence $D|pd$. Thus $d|D|pd$. So, as $p$ is prime, we have $D = d$ or $pd$. □

**Theorem 1.2** (*[10, Theorem 4.6]*). *Let $n = p^2$ where $p$ is an odd prime, and let $y$ be an element from $\mathbb{U}_p$. Then $\mathrm{ord}_p(y) = \mathrm{ord}_n(y)$ if and only if $y^{p-1} \equiv 1 \pmod n$.*

**Proof.** First suppose that $\mathrm{ord}_p(y) = \mathrm{ord}_n(y) = d$. Then $d|(p-1)$ so $p - 1 = dc$ for some integer $c$. As $y^d \equiv 1 \bmod n$), we have $y^{p-1} = y^{dc} = (y^d)^c \equiv 1^c \equiv 1 \pmod n$.

Second, for the converse, suppose that $y^{p-1} \equiv 1 \pmod n$ and that $\mathrm{ord}_p(y) = d$. Then $D = \mathrm{ord}_n(y) = d$ or $pd$. But $y^{p-1} \equiv 1 \pmod n$, so $D|(p-1)$. But $pd$ cannot divide $p - 1$, so $D = d$. □

In the above results, we must always have $d = (p-1)/k$ for some positive integer $k$. If $k = 1$ then $y$ is a primitive root of $p$.

Usually, with the above notation, $\mathrm{ord}_n(y) = dp$. But primes providing exceptions include, for example, $p = 11$, with $\mathrm{ord}_p(3) = \mathrm{ord}_n(3) = \mathrm{ord}_p(9) = \mathrm{ord}_n(9) = (p-1)/2$, and $p = 29$, with $\mathrm{ord}_p(14) = \mathrm{ord}_n(14) = p - 1$. In the present paper we are concerned only with $y = 2$, for which the exceptions are the Wieferich primes [12], of which only two are known [11,8], namely $p = 1093$, for which $\mathrm{ord}_p(2) = \mathrm{ord}_n(2) = (p-1)/3$, and $p = 3511$, for which $\mathrm{ord}_p(2) = \mathrm{ord}_n(2) = (p-1)/2$.

**Lemma 1.2.** *Let $n = p^2$ where $p$ is an odd prime such that $\mathrm{ord}_p(2) = (p-1)/k = t$ and $\mathrm{ord}_n(2) = pt$ for some $k \geqslant 1$. Then, for each $x \in \langle 2\rangle_n$, each of the values $x + pi$, with $1 \leqslant i < p$, is in $\langle 2\rangle_n$, and $\langle 2\rangle_n$, when considered modulo $p$, consists of $p$ copies of $\langle 2\rangle_p$.*

**Proof.** If $x \in \langle 2\rangle_n$ then each of the $\mathbb{Z}_n$-units $x2^{ti}$, $1 \leqslant i < p$, is in $\langle 2\rangle_n$; each is congruent to $x$, modulo $p$, and each is distinct, modulo $n$. □

**Lemma 1.3.** *With $n$ and $p$ as in* Lemma 1.2, *let $y$ be a member of $\mathbb{U}_p$ with $y \notin \langle 2\rangle_p$. Then*

$$\mathbb{U}_p = \langle 2\rangle_p \cup y\langle 2\rangle_p \cup y^2\langle 2\rangle_p \cup \cdots \cup y^{k-1}\langle 2\rangle_p$$

*if and only if*

$$\mathbb{U}_n = \langle 2\rangle_n \cup y\langle 2\rangle_n \cup y^2\langle 2\rangle_n \cup \cdots \cup y^{k-1}\langle 2\rangle_n.$$

**Proof.** This follows immediately from Lemma 1.2. □

Now we give a result about products $pq$ of distinct odd primes $p$ and $q$.

**Lemma 1.4.** *Let $p$ and $q$ be distinct odd primes. Then there exists an integer $i$ such that $2^i \equiv -1 \pmod{pq}$ if and only if the factorisations of $\mathrm{ord}_p(2)$ and $\mathrm{ord}_q(2)$ contain the same positive power of 2.*

**Proof.** Suppose that $\mathrm{ord}_p(2)$ is odd. Then there is no integer $i$ such that $2^i \equiv -1 \pmod p$, and hence no integer $i$ such that $2^i \equiv -1 \pmod{pq}$. So now suppose that $\mathrm{ord}_p(2)$ and $\mathrm{ord}_q(2)$ are both even.

Suppose first that $\mathrm{ord}_p(2) = 2^\alpha u$ and $\mathrm{ord}_q(2) = 2^\alpha v$ where $\alpha \geqslant 1$ and $u, v$ are both odd. Let $w = \mathrm{lcm}(u, v)$. Then $2^{2^{\alpha-1}u} \equiv -1 \pmod p$ and $2^{2^{\alpha-1}v} \equiv -1 \pmod q$, and so $2^{2^{\alpha-1}w} \equiv -1 \pmod{pq}$.

Now suppose that $\mathrm{ord}_p(2) = 2^\alpha u$ and $\mathrm{ord}_q(2) = 2^{\alpha+\beta}v$, where $\alpha \geqslant 1$, $\beta \geqslant 1$ and $u, v$ are both odd. Suppose that $2^k \equiv -1 \pmod{pq}$. Then $2^k \equiv -1 \pmod{p}$ and so $k$ is an odd multiple of $2^{\alpha-1}u$. Similarly $k$ is an odd multiple of $2^{\alpha+\beta-1}v$. This is impossible, as an odd multiple of $2^{\alpha-1}u$ cannot also be an odd multiple of $2^{\alpha+\beta-1}$ unless $\beta = 0$. □

## 2. Theorems for odd primes $n$

In this section, Theorem 2.2 generalises Theorem 2.1. However, we give the special case first, both for clarity and because it is very powerful. Indeed, Theorem 2.1 generalises Theorems 4.6, 5.3 and 5.4 of [2]. Likewise, Theorem 2.3 below generalises Theorem 5.1 of [2]. Our unification and generalisation of earlier results has however necessitated some changes in notation, and terraces obtained from our previous Theorems 5.3 and 5.4 must be reversed and multiplied through by $y^{k-1}$ to give the corresponding terraces obtained from the present Theorem 2.1.

**Theorem 2.1.** *Let $n$ be a prime such that $\mathrm{ord}_n(2) = (n-1)/k$ where $k$ is a positive integer, $k > 1$. Suppose that $i$ is an integer, $1 \leqslant i < \mathrm{ord}_n(2) - 1$, such that $i$ and $\mathrm{ord}_n(2)$ are relatively prime, $2^i - 1 \in \pm\langle 2\rangle$ and $\mathbb{Z}_n\backslash\{0\} = \langle 2, y\rangle$ where $y = (2^{i+1} - 1)^{-1}$. Then*

$$0 \mid 2^{-1}\ 2^{-2}\ \ldots\ 2^0 \mid 2^i y\ 2^{2i} y\ \ldots\ 2^0 y \mid 2^i y^2\ 2^{2i} y^2\ \ldots\ 2^0 y^2 \mid \cdots \mid 2^i y^{k-1}\ 2^{2i} y^{k-1}\ \ldots\ 2^0 y^{k-1}$$

*is a terrace for $\mathbb{Z}_n$. It is a half-and-half terrace if and only if $\mathrm{ord}_n(2)$ is odd.*

**Proof.** Let $\theta = 2^i$; then, as $\gcd(i, \mathrm{ord}_n(2)) = 1$, we have $\mathrm{ord}_n(\theta) = (n-1)/k$ and $\langle\theta\rangle = \langle 2\rangle$. Thus the elements of the proposed terrace are indeed all the elements of $\mathbb{Z}_n$. The differences between elements within segments are all values $2^j$ except $2^{-1}$ and all values $(\theta-1)\theta^j y^l$ except $(\theta-1)y, \ldots, (\theta-1)y^{k-1}$. But the fence differences are $2^{-1}$ and all values $y^l(\theta y - 1)$, $l = 0, 1, \ldots, k-2$. Thus, as $\theta y - 1 = -y(\theta - 1)$, these fence differences are precisely the missing ones. Finally, as $\theta - 1 \in \pm\langle 2\rangle$, these differences, apart from sign, give each element of $\langle 2, y\rangle = \mathbb{Z}_n\backslash\{0\}$ once.

If $\mathrm{ord}_n(2)$ is even, then $-1 \in \langle 2\rangle$ and so the terrace cannot be half-and-half.

If $\mathrm{ord}_n(2)$ is odd, then $k$ is even, say $k = 2h$, and $-1 \in y^h\langle 2\rangle$, so that $y^h = -\theta^u$ for some $u$. Thus, for $i = 2, 3, \ldots, h$, the members of the $(i+h)$th segment are the negatives of the elements of the $i$th segment, and so their differences are the negatives of each other. Finally, the differences in the $(h+1)$th segment are $y^h(\theta-1)\theta^i$, i.e. $-(\theta-1)\theta^{i+u}$, and so they are the elements of $\pm\langle 2\rangle$, and hence are, apart from sign, the same as the differences from the first segment. Thus, if $\mathrm{ord}_n(2)$ is odd, the terrace is half-and-half. □

**Note 2.1(a).** If we can and do take $i = 1$ in Theorem 2.1, we have a form of the "Powers of 2 and 3" method described in [5, Section 5], of which Theorem 4.6 of [2, p. 49] provides a special case with $k = 2$, and Theorems 5.3 and 5.4 of [2, pp. 51–52] provide special cases with $k \geqslant 2$. If we have $i > 1$ in the present Theorem 2.1, the construction of the terrace, from the element $2^0$ onwards, is based on the more general "Powers of $\kappa$ and $2\kappa - 1$" method with $\kappa = 2^i$ [6, Section 3].

**Note 2.1(b).** If $k = 2$ in Theorem 2.1, then $\langle 2\rangle$ is the set of quadratic residues, modulo $n$, and certain special cases arise as follows. Note that if $n \equiv 1 \pmod 4$ then the condition $2^i - 1 \in \pm\langle 2\rangle$ becomes : $2^i - 1$ is a square.

- We can take $i = 1$ if and only if 3 is not a quadratic residue, modulo $n$, i.e. if and only if $n \equiv 7$ or $17 \pmod{24}$, as in Theorem 4.6 of [2, p. 49].
- We can take $i = 2$ if and only if the element 7 (given by $2^3 - 1$) is not a quadratic residue, modulo $n$, and $(n-1)/2$ is odd, i.e. if and only if $n \equiv 15$, 23 or $39 \pmod{56}$.
- We can take $i = 3$ if and only if 2 and 7 are squares, 15 is not a square, and $n \equiv 2 \pmod 3$ , i.e., by quadratic reciprocity arguments, if and only if (i) $n \equiv 23$ or $47 \pmod{120}$, or (ii) $n \equiv 281$, 401, 449, 569, 641 or $809 \pmod{840}$.
- The value $y = 2^j - 1$ cannot arise for any integer $j$ satisfying $1 < j < \mathrm{ord}_n(2)$.
- The value $y = 5$ can arise when neither 3 nor 5 is in $\langle 2\rangle$, e.g. we can take $(n, i, y) = (103, 31, 5)$.
- If $\mathrm{ord}_n(2)$ is odd we can take $y = -2$, $i = \mathrm{ord}_n(2) - 2$.

Table 1
Specimen values of $(i, y)$, where $i > 1$, for Theorem 2.1 for primes $n$ with $\mathrm{ord}_n(2) = (n-1)/2$ and $2 < n < 500$

| $n$ | $\mathrm{ord}_n(2)$ | $i$ | $y$ | $n$ | $\mathrm{ord}_n(2)$ | $i$ | $y$ |
|---|---|---|---|---|---|---|---|
| 7* | 3 | – | – | 239 | 119 | 2 | 205 |
| 17* | 8 | – | – | 263 | 131 | 2 | 188 |
| 23 | 11 | 2 | 10 | 271* | 135 | 13 | 130 |
| 41* | 20 | 13 | 12 | 311 | 155 | 4 | 301 |
| 47 | 23 | 3 | 22 | 313 | 156 | 67 | 90 |
| 71 | 35 | 2 | 61 | 359 | 179 | 2 | 154 |
| 79* | 39 | 2 | 34 | 367* | 183 | 7 | 154 |
| 97 | 48 | 5 | 77 | 383 | 191 | 3 | 332 |
| 103* | 51 | 4 | 10 | 401* | 200 | 3 | 107 |
| 137* | 68 | 21 | 20 | 409 | 204 | 23 | 187 |
| 167 | 83 | 3 | 78 | 449* | 224 | 3 | 30 |
| 191 | 95 | 2 | 82 | 463* | 231 | 2 | 397 |
| 193 | 96 | 23 | 40 | 479 | 239 | 4 | 170 |
| 199* | 99 | 16 | 54 | 487* | 243 | 2 | 348 |

An asterisk * marks values of $n$ for which we can take $(i, y) = (1, 3^{-1})$. The two consecutive $y$-values of 154 are correct.

Table 2
Specimen values of $(i, y)$, where $i > 1$, for Theorem 2.1 for primes $n$ in the range $2 < n < 1000$, with $\mathrm{ord}_n(2) = (n-1)/k$ where $k > 2$

| $n$ | $k$ | $\mathrm{ord}_n(2)$ | $i$ | $y$ | $n$ | $k$ | $\mathrm{ord}_n(2)$ | $i$ | $y$ |
|---|---|---|---|---|---|---|---|---|---|
| 31* | 6 | 5 | – | – | 439† | 6 | 73 | 3 | 322 |
| 43* | 3 | 14 | – | – | 457† | 6 | 76 | 67 | 318 |
| 73† | 8 | 9 | – | – | 499 | 3 | 166 | 5 | 301 |
| 89* | 8 | 11 | – | – | 571* | 5 | 114 | 37 | 534 |
| 109* | 3 | 36 | 23 | 57 | 577† | 4 | 144 | 5 | 403 |
| 113* | 4 | 28 | 25 | 74 | 593*† | 4 | 148 | 5 | 433 |
| 127* | 18 | 7 | – | – | 601 | 24 | 25 | – | – |
| 151* | 10 | 15 | – | – | 617*† | 4 | 154 | 61 | 244 |
| 157* | 3 | 52 | 3 | 21 | 631* | 14 | 45 | 37 | 471 |
| 223*† | 6 | 37 | 16 | 122 | 641*† | 10 | 64 | 41 | 429 |
| 229* | 3 | 76 | 13 | 205 | 643 | 3 | 214 | 7 | 58 |
| 233* | 8 | 29 | 6 | 222 | 673† | 14 | 48 | – | – |
| 241† | 10 | 24 | – | – | 683* | 31 | 22 | – | – |
| 251* | 5 | 50 | 23 | 83 | 691* | 3 | 230 | 27 | 656 |
| 257* | 16 | 16 | – | – | 727† | 6 | 121 | 20 | 581 |
| 277* | 3 | 92 | 29 | 229 | 733* | 3 | 244 | 15 | 214 |
| 281* | 4 | 70 | 19 | 12 | 739* | 3 | 246 | 7 | 597 |
| 283* | 3 | 94 | 17 | 10 | 811* | 3 | 270 | 17 | 636 |
| 307 | 3 | 102 | 11 | 62 | 881* | 16 | 55 | – | – |
| 331* | 11 | 30 | – | – | 911† | 10 | 91 | 88 | 606 |
| 337† | 16 | 21 | – | – | 919† | 6 | 153 | 92 | 557 |
| 353*† | 4 | 88 | 25 | 107 | 937† | 8 | 117 | 73 | 749 |
| 397* | 9 | 44 | – | – | 953* | 14 | 68 | 9 | 177 |
| 431† | 10 | 43 | 2 | 308 | 971* | 5 | 194 | 3 | 259 |
| 433† | 6 | 72 | 65 | 377 | 997 | 3 | 332 | 5 | 364 |

An asterisk * marks $n$-values for which we can take $(i, y) = (1, 3^{-1})$; a dagger † marks $n$-values also covered in Table 3 for Theorem 2.3.

**Note 2.1(c).** For primes $n$ with $\mathrm{ord}_n(2) = (n-1)/2$ and $2 < n < 500$, Table 1 gives specimen values of $(i, y)$, $i > 1$, for terraces obtainable from Theorem 2.1. Likewise, Table 2 gives specimen values for $\mathrm{ord}_n(2) = (n-1)/k$ with $k > 2$ and $2 < n < 1000$.

**Example 2.1(a).** For $n = 23$ we have $k = 2$ and $\mathrm{ord}_n(2) = 11$; we can take $i = 2$, 3, 5, 8 or 9. For $i = 2$ we have $y = 7^{-1} = 10$, which gives us the quasi-segregated $\mathbb{Z}_{23}$ terrace

$$0 \;|12\;\; 6\;\; 3\;\; 13\;\; 18\;\; 9\;\; 16\;\; 8\;\; 4\;\; 2\;\; 1\;|\;17\;\; 22\;\; 19\;\; 7\;\; 5\;\; 20\;\; 11\;\; 21\;\; 15\;\; 14\;\; 10.$$

**Example 2.1(b).** For $n = 31$ we have $k = 6$ and $\mathrm{ord}_n(2) = 5$. We can take $i = 1$ only (see Table 2), whence $y = 21$. This yields the $\mathbb{Z}_{31}$ terrace which, when reversed and multiplied through by $y^{-(k-1)} = 26$, becomes the $\mathbb{Z}_{31}$ terrace from Theorem 5.3 of [2, p. 51].

**Example 2.1(c).** For $n = 79$ we have $k = 2$ and $\mathrm{ord}_n(2) = 39$. We can take $i = 1$ to obtain the $\mathbb{Z}_{79}$ terrace that arises from Theorem 4.6 of [2, p. 49]. As Note 2.1(b) indicates, we can also take $i = 2$ (see Table 1).

**Example 2.1(d).** For $n = 109$ we have $k = 3$ and $\mathrm{ord}_n(2) = 36$. We can take $i = 1$ to obtain the $\mathbb{Z}_{109}$ terrace which, if reversed and multiplied through by $y^{-(k-1)} = 9$, yields the $\mathbb{Z}_{109}$ terrace from Theorem 5.4 of [2, p. 52]. We can also take $i = 23$ and $y = 44^{-1} = 57$ (see Table 2) to give the $\mathbb{Z}_{109}$ terrace

$$0 \;|\; 55\;\; 82\;\; 41\;\; \ldots\;\; 4\;\; 2\;\; 1 \;|\; 29\;\; 53\;\; 48\;\; \ldots\;\; 14\;\; 97\;\; 57 \;|\; 18\;\; 78\;\; 11\;\; \ldots\;\; 35\;\; 79\;\; 88.$$

**Theorem 2.2.** *Let $n$ be a prime such that $\mathrm{ord}_n(2) = (n-1)/k$ where $k$ is a positive integer, $k > 1$. Suppose that the integers $i_j$, not necessarily all distinct, are such that*

(i) $1 \leqslant i_j < \mathrm{ord}_n(2) - 1$;
(ii) *$i_j$ and $\mathrm{ord}_n(2)$ are mutually prime*;
(iii) $2^{i_j} - 1 \in \pm\langle 2\rangle$; *and*
(iv) $\mathbb{Z}_n\backslash\{0\} = \langle 2, y_j\rangle$ *where* $y_j = (2^{i_j+1} - 1)^{-1}$.

*Suppose further that $y_1\langle 2\rangle = y_2\langle 2\rangle = \cdots = y_{k-1}\langle 2\rangle$. Write $z_j = y_1 y_2 \cdots y_j$ for $j = 1, 2, \ldots, k-1$. Then*

$$0 \;|\; 2^{-1}\;\; 2^{-2}\ldots\;\; 2^0 \;|\; 2^{i_1}z_1\;\; 2^{2i_1}z_1\ldots\;\; 2^0 z_1 \;|\; 2^{i_2}z_2\;\; 2^{2i_2}z_2\ldots\;\; 2^0 z_2 \;|$$
$$\cdots \;|\; 2^{i_{k-1}}z_{k-1}\;\; 2^{2i_{k-1}}z_{k-1}\ldots\;\; 2^0 z_{k-1}$$

*is a terrace for $\mathbb{Z}_n$. It is a half-and-half terrace if and only if $\mathrm{ord}_n(2)$ is odd.*

**Proof.** Let $x_j = 2^{i_j}$ for $j = 1, 2, \ldots, k-1$. The first missing difference and first fence difference are both $2^{-1}$. Thereafter, the missing differences are $z_j(x_j - 1)$ and the fence differences are $z_{j-1}(y_j x_j - 1)$. But $z_j(x_j - 1) = z_{j-1}y_j(x_j - 1) = -z_{j-1}(y_j x_j - 1)$, since $y_j = 1/(2x_j - 1)$, so, as in Theorem 2.1, the differences give, apart from sign, all elements of $\mathbb{Z}_n\backslash\{0\}$ once. The proof of the half-and-half property is as for Theorem 2.1. □

**Example 2.2(a).** For $n = 157$ we have $k = 3$ and $\mathrm{ord}_n(2) = 52$. We can take $i_1 = 3$ (with $y_1 = 15^{-1} = 21$) and $i_2 = 15$ (with $y_2 = 66^{-1} = 69$), there being no need for $y_1$ and $y_2$ to be relatively prime. We then obtain the $\mathbb{Z}_{157}$ terrace

$$0 \;|\; 79\;\; 118\;\; 59\ldots\;\; 4\;\; 2\;\; 1 \;|\; 11\;\; 88\;\; 76\ldots\;\; 96\;\; 140\;\; 21 \;|\; 107\;\; 52\;\; 15\ldots\;\; 37\;\; 62\;\; 36.$$

Alternatively, we can interchange $i_1$ and $i_2$ (and therefore also $y_1$ and $y_2$) to obtain the $\mathbb{Z}_{157}$ terrace

$$0 \;|\; 79\;\; 118\;\; 59\ldots\;\; 4\;\; 2\;\; 1 \;|\; 35\;\; 152\;\; 68\ldots\;\; 84\;\; 145\;\; 69 \;|\; 131\;\; 106\;\; 63\ldots\;\; 30\;\; 83\;\; 36.$$

**Example 2.2(b).** For $n = 439$ we have $k = 6$ and $\mathrm{ord}_n(2) = 73$. We can take each of $i_1, i_2, \ldots, i_5$ to be any one of 3, 21, 26, 53 or 61. Of these $i$-values, 3, 26 and 53 satisfy $2^i - 1 \in +\langle 2\rangle$, whereas 21 and 61 satisfy $2^i - 1 \in -\langle 2\rangle$.

**Corollary 2.1.** *If all the elements in the terrace in Theorem* 2.1 *or Theorem* 2.2 *are written so as to lie in the interval $[0, n-1]$ and the zero element is then omitted, the sequence that remains is a terrace for $\mathbb{Z}_{n-1}$, with the zero element of $\mathbb{Z}_{n-1}$ written as $n-1$ (cf.* [6]).

Table 3
Specimen solutions $(i, y, c)$, $y^h \in \mathscr{S}$, $h > 1$, for Theorem 2.3 for primes $n$ in the range $2 < n < 1000$; here $\mathrm{ord}_n(2) = (n-1)/k$ where $k = 2h$

| $n$ | $k$ | $\mathrm{ord}_n(2)$ | $i$ | $y$ | $c$ | $n$ | $k$ | $\mathrm{ord}_n(2)$ | $i$ | $y$ | $c$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 73† | 8 | 9 | 1 | 49 | 7 | 577 | 4 | 144 | 47 | 263 | 5 |
| 223 | 6 | 37 | 8 | 199 | −1 | 593 | 4 | 148 | 15 | 35 | 3 |
| 241† | 10 | 24 | 1 | 161 | 7 | 617 | 4 | 154 | 17 | 158 | 3 |
| 337† | 16 | 21 | 1 | 225 | 5 | 641 | 10 | 64 | 25 | 285 | 3 |
| 353 | 4 | 88 | 21 | 197 | 3 | 673† | 14 | 48 | 1 | 449 | 5 |
| 431 | 10 | 43 | 13 | 345 | −1 | 727 | 6 | 121 | 81 | 556 | −1 |
| 433 | 6 | 72 | 1 | 289 | 5 | 911 | 10 | 91 | 4 | 529 | −1 |
| 439 | 6 | 73 | 30 | 211 | −1 | 919 | 6 | 153 | 43 | 482 | −1 |
| 457 | 6 | 76 | 1 | 305 | 5 | 937 | 8 | 117 | 88 | 441 | 5 |

A dagger † marks an $n$-value not covered by Theorem 2.1.

**Theorem 2.3.** *Let $n$ be a prime such that $\mathrm{ord}_n(2) = (n-1)/2h$ where $h$ is a positive integer, $h > 1$. Suppose that $i$ is an integer, $1 \leqslant i < \mathrm{ord}_n(2) - 1$, such that $i$ and $\mathrm{ord}_n(2)$ are relatively prime and $2^i - 1 \in \pm\langle 2\rangle$. Write $y = (2^{i+1} - 1)^{-1}$. Suppose further that the sets $\{y^s\langle 2\rangle\}$ $(s = 0, 1, \ldots, h-1)$ are disjoint. Write $\mathscr{S} = \bigcup_{s=0}^{h-1} y^s\langle 2\rangle$, and let $c$ be an integer such that $\mathbb{Z}_n\backslash\{0\} = \mathscr{S} \cup c\mathscr{S}$. Write*

$$\mathbf{A} = 2^{-1}\ 2^{-2}\ldots\ 2^0 \mid 2^i y\ 2^{2i} y\ldots\ 2^0 y \mid 2^i y^2\ 2^{2i} y^2\ldots\ 2^0 y^2 \mid \cdots \mid 2^i y^{h-1}\ 2^{2i} y^{h-1}\ldots\ 2^0 y^{h-1}.$$

*Then*

$$c\mathbf{A}^{\mathrm{rev}} \mid 0 \mid \mathbf{A}$$

*is a terrace for $\mathbb{Z}_n$. The terrace is narcissistic if and only if $c = -1$. The terrace is segregated if and only if $y$ is a square in $\mathbb{Z}_n$.*

**Proof.** If $a^h \notin \langle 2\rangle$ we can take $c = a^h$; if $a^h \in \langle 2\rangle$ then take any $c \notin S$. Again set $\theta = 2^i$. On the right of 0, the missing differences are, apart from sign, $2^{-1}$ and $(\theta - 1)y^j$, $j = 1, 2, \ldots, h-1$. The fence differences are $2^{-1}$ and $(\theta y - 1)y^k$, $k = 0, 1, \ldots, h-2$. But $y(\theta - 1) = -(y\theta - 1)$, so the fence differences compensate for the missing differences. As $\theta - 1 \in \langle 2\rangle$, the differences are precisely all the elements of $\mathscr{S}$. Similarly for the differences on the left of 0. □

**Note 2.3(a).** A terrace given by Theorem 2.3 is half-and-half whenever both $h$ and $\mathrm{ord}_n(2)$ are odd. It may or may not be half-and-half if $h$ is even and $\mathrm{ord}_n(2)$ is odd; for example, if $n = 89$ we have $h = 4$ and $\mathrm{ord}_n(2) = 11$, and the terrace with $i = 1$ and $y = 30$ is half-and-half.

**Note 2.3(b).** For any $n$-value covered by Theorem 2.3, the admissible values of $i$ include all those $i$-values that satisfy Theorem 2.1. The other admissible $i$-values for Theorem 2.3 are such that the corresponding $y$-values satisfy $y^h \in \mathscr{S}$, so that $\langle 2, y\rangle$ contains half the elements of $\mathbb{Z}_n\backslash\{0\}$; specimens of such $i$-values are given in Table 3. For such $i$-values, three cases can be distinguished:

(i) $\mathrm{ord}_n(2)$ and $h$ are both odd: here $-1 \notin \langle 2, y\rangle$, and a narcissistic terrace for $\mathbb{Z}_n$ can be obtained by taking $c = -1$.
(ii) $\mathrm{ord}_n(2)$ is odd and $h$ is even: here $-1 \notin \langle 2\rangle$ but $-1 \in \langle 2, y\rangle$, so we cannot take $c = -1$.
(iii) $\mathrm{ord}_n(2)$ is even: here $-1 \in \langle 2\rangle$, so we again cannot take $c = -1$.

**Note 2.3(c).** Table 3 contains six $n$-values satisfying $n \equiv 1 \pmod{24}$. For each of these we can take $i = 1$, as each has just half of the elements of $\mathbb{Z}_n\backslash\{0\}$ lying in $\langle 2, 3\rangle$.

**Note 2.3(d).** Theorem 2.3 can be generalised in the same way that we generalised Theorem 2.1 to Theorem 2.2, but we omit details as they provide little new insight.

**Example 2.3(a)** ($\mathrm{ord}_n(2)$ *and h both odd*). For $n = 223$, $h = 3$, $\mathrm{ord}_n(2) = 37$ we can take $i = 8$ and $y = 65^{-1} = 199$. Then $-1 \notin \langle 2, y\rangle$ and $\mathbb{Z}_n\backslash\{0\} = \langle 2, y\rangle \cup -\langle 2, y\rangle$. So we can take $c = -1$ to obtain a narcissistic terrace for $\mathbb{Z}_{223}$, with

$$\mathbf{A} = 112\ \ 56\ \ 28 \ldots\ \ 4\ \ 2\ \ 1 \mid 100\ \ 178\ \ 76 \ldots\ \ 121\ \ 202\ \ 199 \mid 53\ \ 188\ \ 183 \ldots\ \ 218\ \ 58\ \ 130.$$

**Example 2.3(b)** ($\mathrm{ord}_n(2)$ *odd but h even*). For $n = 937$, $h = 8$, $\mathrm{ord}_n(2) = 117$ we have $-1 \notin \langle 2\rangle$. However we can take $i = 88$ and $y = 17^{-1} = 441$. Then $-1 \in \langle 2, y\rangle$ where $\langle 2, y\rangle$ constitutes half of $\mathbb{Z}_n\backslash\{0\}$. As $\mathbb{Z}_n\backslash\{0\} = \langle 2, y\rangle \ \cup\ 5\langle 2, y\rangle$, we can take $c = 5$ to obtain a non-narcissistic terrace for $\mathbb{Z}_{937}$.

**Example 2.3(c)** ($\mathrm{ord}_n(2)$ *even*). For $n = 353$, $h = 2$, $\mathrm{ord}_n(2) = 88$ we now have $-1 \in \langle 2\rangle$. We can take $i = 21$ and $y = 310^{-1} = 197$. Then $\langle 2, y\rangle$ again constitutes half of $\mathbb{Z}_n\backslash\{0\}$. As we now have $\mathbb{Z}_n\backslash\{0\} = \langle 2, y\rangle \ \cup\ 3\langle 2, y\rangle$, we can take $c = 3$ to obtain a non-narcissistic terrace for $\mathbb{Z}_{353}$.

**Theorem 2.4.** *Let n be a prime such that* $\mathrm{ord}_n(2) = (n-1)/k$ *where k is a positive integer*, $k > 1$, *and* $\mathrm{ord}_n(2)$ *is even. Suppose that i is an integer*, $1 \leqslant i < \mathrm{ord}_n(2) - 1$, *such that i and* $\mathrm{ord}_n(2)$ *are mutually prime*, $2^i - 1 \in \langle 2\rangle$ *and* $\mathbb{Z}_n\backslash\{0\} = \langle 2, y\rangle$ *where* $y = (2^{i+1} - 1)^{-1}$. *Write*

$$\mathbf{A} = : +2^{-1}\ \ +2^{-2} \ldots\ \ -2^0 : \mid : -2^i y\ \ -2^{2i} y\ \ \ldots\ \ +2^0 y : \mid : +2^i y^2\ \ +2^{2i} y^2 \ldots\ \ -2^0 y^2 : \mid$$
$$\cdots \mid : 2^i(-y)^{k-1}\ \ 2^{2i}(-y)^{k-1} \ldots\ \ -2^0(-y)^{k-1} : .$$

*Then*

$$-\mathbf{A}^{\mathrm{rev}} \mid 0 \mid \mathbf{A}$$

*is a narcissistic terrace for* $\mathbb{Z}_n$.

**Proof.** Similar to previous proofs. □

**Note 2.4(a).** For any $n$-value covered by Theorem 2.4, the admissible values of $i$ are the same as those for Theorem 2.1.

**Note 2.4(b).** Theorem 2.4 can be generalised in the same way as Theorems 2.1 and 2.3 can, but we again omit details.

**Example 2.4.** For $n = 41$ we have $k = 2$ and $\mathrm{ord}_n(2) = 20$. We can take $i = 13$ (as in Table 1), with $y = 24^{-1} = 12$. Thus Theorem 2.4 gives us a $\mathbb{Z}_{41}$ terrace

$$\mathbf{A} = : 21\ \ 31\ \ 36\ \ 18\ \ 9\ \ 25\ \ 33\ \ 37\ \ 39\ \ 40 : \mid :\ \ 14\ \ 11\ \ 35\ \ 7\ \ 26\ \ 38\ \ 24\ \ 13\ \ 19\ \ 12 : .$$

The above theorems yield $\mathbb{Z}_n$ terraces for all odd primes less than 1000, excepting $n = 601$ for which $\mathrm{ord}_n(2)$ has the small value 25. For $n = 601$ the only $i$-value from $\{1, 2, \ldots, 23\}\backslash\{5, 10, 15, 20\}$ that has $2^i - 1 \in \pm\langle 2\rangle \pmod{601}$ is $i = 1$, which gives $2^{i+1} - 1 = 3$; thus, as $|\langle 2, 3, \rangle| = 75$, no $i$-value is available that meets even the conditions of Theorem 2.3. However, power-sequence terraces for $\mathbb{Z}_{601}$ can be obtained from the special case $\alpha = \beta = -1$ of Theorem 4.2 of [2]. (This special case yields $\mathbb{Z}_n$ terraces for some values $n$ that are congruent to $\pm 1$, modulo 10.) One such $\mathbb{Z}_{601}$ terrace is obtained from powers of the primitive root $w = 137$ of 601, with $w^2 = w + 1 = w^{-1} + 2$, and is

$$1\ \ w^2\ \ w^4 \ldots\ \ w^{-2} \mid 0 \mid w^{-1}\ \ w^1\ \ w^3 \ldots\ \ w^{-3}$$

i.e.

$$1\ \ 138\ \ 413 \ldots\ \ 466 \mid 0 \mid 136\ \ 137\ \ 275 \ldots\ \ 271.$$

Other such terraces are similarly obtained by taking $w = -137$, $137^{-1}$ or $-137^{-1} \pmod{601}$.

## 3. Theorems for $n = p^2$ where $p$ is an odd prime

We now give a theorem that provides $\mathbb{Z}_n$ terraces, $n = p^2$, where $p$ is an odd prime but not a Wieferich prime (see Section 1.2 above). The scope of this theorem is much wider than that of Theorems 6.3 and 6.4 of [2, p. 54].

**Theorem 3.1.** *Let $n = p^2$ where $p$ is an odd prime such that $\mathrm{ord}_p(2) = (p-1)/k$ and $\mathrm{ord}_n(2) = (n-p)/k$ where $k$ is a positive integer, $k > 1$. Suppose that $i$ is an integer, $1 \leqslant i < \mathrm{ord}_n(2) - 1$, such that $i$ and $\mathrm{ord}_n(2)$ are mutually prime, $2^i - 1 \in \pm\langle 2\rangle \pmod n$, and $\mathbb{U}_n = \langle 2, y\rangle \pmod n$ where $y \equiv (2^{i+1} - 1)^{-1} \pmod n$. Let $\mathbf{B}$ be a sequence of elements of $\mathbb{Z}_p \backslash \{0\}$ such that*

$$\mathbf{B} \mid 0$$

*is a terrace for $\mathbb{Z}_p$. Write*

$$\mathbf{A} = 2^{-1}\ 2^{-2} \dots\ 2^0 \mid 2^i y\ 2^{2i} y \dots\ 2^0 y \mid 2^i y^2\ 2^{2i} y^2 \dots\ 2^0 y^2 \mid \cdots \mid 2^i y^{k-1}\ 2^{2i} y^{k-1} \dots\ 2^0 y^{k-1}.$$

*Then*

$$p\mathbf{B} \mid 0 \mid \mathbf{A}$$

*is a terrace for $\mathbb{Z}_n$. The values of $i$ that meet the required conditions comprise precisely the values $i' + j\,\mathrm{ord}_p(2)$ $(j = 0, 1, \dots, p-1)$ that are coprime with $\mathrm{ord}_n(2)$ (i.e. that are not multiples of $p$), where $i'$ is a value of $i$ satisfying the conditions of Theorem 2.1 when that theorem is applied to the prime $p$.*

**Proof.** As $2^i - 1 \in \pm\langle 2\rangle_n$, the difference $2^{(j+1)i} y^l - 2^{ji} y^l = (2^i - 1)2^{ji} y^l$ is in $\pm y^l \langle 2\rangle_n$. The missing differences are $2^{-1}$ and $(2^i - 1)y^l$, $1 \leqslant l \leqslant k-1$, and the fence differences are $2^{-1}$ and $(2^i y - 1)y^l$, $0 \leqslant l \leqslant k-2$. As $2^i y - 1 = -y(2^i - 1)$, these fence differences compensate for the missing ones. Thus the sequence is a $\mathbb{Z}_n$ terrace.

If $2^i - 1 \in \pm\langle 2\rangle_n$ then $2^i - 1 \in \pm\langle 2\rangle_p$ and so $i = i' + tj$ for some $i'$, $j$. Conversely, suppose that $2^{i'} - 1 \in \pm\langle 2\rangle_p$; we show that each $2^{i'+tj} \in \pm\langle 2\rangle_n$. Suppose that $2^t = 1 + \lambda p$ and $2^{i'} - 1 = \pm 2^\alpha + lp$. Then

$$\begin{aligned} 2^{i'+tj} - 1 = 2^{i'}(1 + \lambda p)^j - 1 &\equiv 2^{i'}(1 + \lambda jp) - 1 \pmod n \\ &\equiv \pm 2^\alpha + p(l + 2^{i'}\lambda j) \equiv \pm 2^\alpha \pmod n \end{aligned}$$

if we choose $j$ so that $2^{i'}\lambda j \equiv -l \pmod p$. Accordingly, there exists a value $j$ such that $2^{i'+tj} - 1 \in \pm\langle 2\rangle_n$. But if $2^\mu - 1 \in \pm\langle 2\rangle_n$, say $2^\mu - 1 \equiv \pm 2^\beta \pmod n$, then

$$2^{\mu+t} - 1 = 2^t(2^\mu - 1) + (2^t - 1) \equiv \pm 2^{t+\beta} + \lambda p \pmod n$$

and so, by Lemma 1.2, we have $2^{\mu+t} - 1 \in \pm\langle 2\rangle_n$. So from $2^{i'+jt} - 1 \in \pm\langle 2\rangle_n$ we conclude that $2^{i'+jt} \in \pm\langle 2\rangle_n$ for each $j$. □

**Note 3.1.** Theorem 3.1can be generalised in the same way as Theorems 2.1 and 2.3 can, but again we consider the details to be insufficiently exciting for presentation.

**Example 3.1(a).** For $n = 49$, $p = 7$, we have $\mathrm{ord}_{49}(2) = (n - p)/2 = 21$. The successive powers of 2, modulo 49, are

1 2 4 8 16 32 15 30 11 22 44 39 29 9 18 36 23 46 43 37 25.

The only possible value of $i'$ for Theorem 3.1 is 1, so we have the $i$-values $1 + j\,\mathrm{ord}_p(2) = 1 + 3j$, where $j = 0$, 1, 3, 4, 5 or 6, the value $j = 2$ being excluded as it gives $1 + 3j = 7$, which is a factor of $\mathrm{ord}_{49}(2)$. Thus we can take

$$(i, y) = (1, 33),\ \ (4, 19),\ \ (10, 40),\ \ (13, 26),\ \ (16, 12)\ \text{ or }\ (19, 47).$$

With $(i, y) = (1, 33)$, one of the $\mathbb{Z}_{49}$ terraces obtainable from Theorem 3.1 is

$$35\ \ 42\ \ 21\ \mid\ 7\ \ 14\ \ 28\ \mid\ 0\ \mid\ 25\ \ 37\ \ 43\ldots\ \ 4\ \ 2\ \ 1\ \mid\ 17\ \ 34\ \ 19\ldots\ \ 45\ \ 41\ \ 33;$$

when multiplied through by 3, this gives the $\mathbb{Z}_{49}$ terrace obtainable from Theorem 6.4 of [2, p. 54]. With $(i, y) = (4, 19)$, another of the $\mathbb{Z}_{49}$ terraces obtainable from Theorem 3.1 is

$$28\ \ 14\ \ 7\ \mid\ 35\ \ 21\ \ 42\ \mid\ 0\ \mid\ 25\ \ 37\ \ 43\ldots\ \ 4\ \ 2\ \ 1\ \mid\ 10\ \ 13\ \ 12\ldots\ \ 24\ \ 41\ \ 19$$

the choice of **B** here is such that the terrace is also obtainable from Corollary 3.1 below, so the terrace can be converted into a half-and-half terrace by moving the last segment to the start.

**Example 3.1(b).** For $n = 289$, $p = 17$, we have $\mathrm{ord}_{289}(2) = (n - p)/2 = 136$. Again, the only possible value of $i'$ for Theorem 3.1 is 1, so we have the $i$-values $1 + j\ \mathrm{ord}_p(2) = 1 + 8j$, where $j = 0, 1, 3, 4, \ldots, 16$, the value 2 again being excluded. Taking $i = 1$ gives $(i, y) = (1, 193)$, from which we can obtain the $\mathbb{Z}_{289}$ terrace that arises from Theorem 6.3 of [2, p. 54], namely

$$102\ \ 51\ldots\ \ 204\ \mid\ 17\ \ 34\ldots\ \ 153\ \mid\ 0\ \mid\ 145\ \ 217\ldots\ \ 1\ \mid\ 97\ \ 194\ldots\ \ 193.$$

**Example 3.1(c).** For $n = 529$, $p = 23$, we have $\mathrm{ord}_{529}(2) = (n - p)/2 = 253$. The possible values of $i'$ for Theorem 3.1 are 2, 3, 5, 8 and 9 (see Example 2.1(a)). If we try, for example, taking $i' = 2$ in conjunction with $j = 4$, we obtain $i = i' + j\ \mathrm{ord}_{23}(2) = 46$, which is not coprime with $\mathrm{ord}_n(2)$. But if, for example, we choose $i' = 3$, $j = 2$, we obtain $i = i' + j\ \mathrm{ord}_{23}(2) = 3 + 22 = 25$; then, as $2^{26} - 1 = 452$, we can obtain a $\mathbb{Z}_{529}$ terrace by using $y = 452^{-1} = 158$.

**Example 3.1(d).** For $n = 961$, $p = 31$, we have $\mathrm{ord}_{961}(2) = (n - p)/6 = 155$. The only possible value of $i'$ for Theorem 3.1 is 1, so we can choose from the $i$-values $1 + j\ \mathrm{ord}_p(2) = 1 + 5j$ ($j = 0, 1, \ldots, 5, 7, 8, \ldots, 30$). Taking $i = 6$ gives $y = 734$.

**Corollary 3.1.** *Let $n = p^2$ where $p$ is an odd prime such that $p \equiv 7$ or $17 \pmod{24}$, with $\mathrm{ord}_p(2) = (p - 1)/2$ and $\mathrm{ord}_n(2) = (n - p)/2$. Let $i$ be any integer such that $(i - 1)/\mathrm{ord}_p(2) \in \{1, 3, 4, 5, \ldots, p - 1\}$ and $2^i - 1 \in \pm\langle 2\rangle_p$. Write $y = (2^{i+1} - 1)^{-1}$ and let $x$ be a multiple of $p$ but not of $n$. Then, if $y \notin \langle 2\rangle_p$, the sequence*

$$2^0x\ \ 2^{-1}x\ \ 2^{-2}x\ldots\ \ 2^1x\ \mid\ 3\cdot 2^0x\ \ 3\cdot 2^1x\ \ 3\cdot 2^2x\ldots\ \ 3\cdot 2^{-1}x\ \mid\ 0\ \mid\ 2^{-1}\ \ 2^{-2}\ldots\ \ 2^0\ \mid\ 2^iy\ \ 2^{2i}y\ldots\ \ 2^0y$$

*of elements of $\mathbb{Z}_n$ is a terrace for $\mathbb{Z}_n$. If $x \equiv -2(2^{i-1} - 1) \pmod{n}$ and the final segment is moved to the start, then the resulting sequence is also a terrace, which is a half-and-half terrace if $p \equiv 7 \pmod{24}$.*

**Proof.** As $\mathrm{ord}_p(2) = (p - 1)/2$, the element 2 is a square modulo $p$ and so we must have $p \equiv 1$ or $7 \pmod 8$. The stronger condition $p \equiv 7$ or $17 \pmod{24}$ ensures that $p \equiv 5$ or $7 \pmod{12}$, so that the element 3 is not a square modulo $p$. Thus $\mathbb{U}_p = \langle 2\rangle \cup 3\langle 2\rangle$.

In Theorem 3.1 take **B** to be

$$2^0\ \ 2^{-1}\ \ \ldots\ \ 2^1\ \mid\ 3\cdot 2^0\ \ 3\cdot 2^1\ \ \ldots\ \ 3\cdot 2^{-1}$$

multiplied by $c$ where $x = cp$. The choice of $i$ ensures, as required by Theorem 3.1, that $i$ is not a multiple of $p$, so the sequence in the statement of the corollary is a terrace.

When the final segment is moved to the front, the fence difference $2^iy - 1$ is lost but the fence difference $x - y$ is gained. But $x - y = -y(2^i - 1) = 2^iy - 1$, so the resulting sequence is a terrace.

Finally suppose that $p \equiv 7 \pmod{24}$, so that $-1$ is not a square, modulo $p$. In each half of the final terrace there is one segment of units and one of multiples of $p$. Suppose that $2^{i+1}x - 2^ix \equiv \pm(2^{j+1}x - 2^jx) \pmod n$. Then $2^i \equiv \pm 2^j \pmod p$, whence $2^i \equiv -2^j \pmod p$. This implies that $-1 \in \langle 2\rangle$ and hence that $-1$ is a square, which gives us a contradiction. A similar argument holds for the other segments, so the final $\mathbb{Z}_n$ terrace is a half-and-half terrace. □

## 4. Theorems for $n = pq$ where $p, q$ are primes $> 3$

Our next theorem, Theorem 4.1, with $n = pq$, uses the methodology of the present paper to generalise the methodology of [5, Section 5.3], which required $p$ and $q$ to be distinct primes each having 2 as a primitive root and which considered only the case $i = 1$. For direct comparison with terraces obtained from Theorem 4.1, the terraces in [5, Section 5.3] must be multiplied through by $2^{-1}$. Interpretation of condition (iii) of Theorem 4.1 requires us to recall Lemma 1.4 above, which establishes that $\langle 2\rangle_n = -\langle 2\rangle_n$ if and only if the factorisations of $\mathrm{ord}_p(2)$ and $\mathrm{ord}_q(2)$ contain the same power of 2.

**Theorem 4.1.** *Let $n = pq$ where $p$ and $q$ are distinct primes both greater than 3. Let $k$ be the integer such that $\mathrm{ord}_n(2) = (p-1)(q-1)/k$. Suppose that $i$ is an integer such that*

(i) $1 \leqslant i < \mathrm{ord}_n(2) - 1$;
(ii) *$i$ and $\mathrm{ord}_n(2)$ are coprime*;
(iii) $2^i - 1 \in \pm\langle 2\rangle$, *modulo $n$*;
(iv) $\mathbb{U}_n = \langle 2, y\rangle_n$ *where* $y = (2^{i+1} - 1)^{-1}$, *modulo $n$*; *and*
(v) $y^{k-1} \pm 2^{-1}$, *modulo $n$, is a multiple $xp$ of $p$*.

*Let* $\mathbf{P}$ *be a sequence of the elements of $\mathbb{Z}_p\backslash\{0\}$ such that $\mathbf{P} \mid 0$ is a terrace for $\mathbb{Z}_p$. Let* $\mathbf{Q}$ *be a sequence of the elements of $\mathbb{Z}_q\backslash\{0\}$ such that $\mathbf{Q} \mid 0$ is a terrace for $\mathbb{Z}_q$ and such that 1 is the first element of* $\mathbf{Q}$. *Then*

$$2^{-1}\ 2^{-2} \ldots\ 2^0 \mid 2^i y\ 2^{2i} y \ldots\ 2^0 y \mid 2^i y^2\ 2^{2i} y^2 \ldots\ 2^0 y^2 \mid \cdots \mid 2^i y^{k-1}\ 2^{2i} y^{k-1} \ldots\ 2^0 y^{k-1} \mid xp\mathbf{Q} \mid 0 \mid q\mathbf{P}^{\mathrm{rev}}$$

*is a terrace for $\mathbb{Z}_n$.*

**Proof.** The missing differences in the units segments are $2^{-1}$ and $(2^i - 1)y^j$, $1 \leqslant j < k$. The fence differences are $(2^i y - 1)y^l$, $0 \leqslant l < k - 1$, and $xp - y^{k-1}$. As $(2^i - 1)y = -(2^i y - 1)$, the fence differences compensate for the missing differences provided that $y^{k-1} \pm 2^{-1} \equiv xp \pmod n$. As $y \notin \langle 2\rangle_n$, the multiplier $x$ is not a multiple of $q$. The differences in the other segments are easily checked. □

**Note 4.1(a).** If $5 \mid n$, $k = 2$ and $3 \notin \langle 2\rangle$, modulo $n$, then Theorem 4.1 provides a $\mathbb{Z}_n$ terrace with $p = 5$, $i = 1$, $y = 3^{-1}$ and $x = 3^{-1} \cdot 2^{-1} \pmod q$.

**Note 4.1(b).** For the range $2 < n < 500$, Table 4 gives specimen parameter-sets for terraces obtainable from Theorem 4.1. Methodology very different from that of the present paper was used in [4, pp. 40–50] to obtain $\mathbb{Z}_n$ terraces for the $n$-values in the present Table 4, $n < 300$, and in [5] for all but two of the present $n$-values, $n < 200$.

**Example 4.1.** For $n = 35$ we have $k = 2$, and Theorem 4.1 yields terraces with $i = 1$ only, with $y = 3^{-1} = 12$, $p = 5$, $q = 7$, $x = 6$. These terraces include the following, for which $\mathbf{P}$ and $\mathbf{Q}$ are obtained by obvious power-sequence constructions:

$$18\ 9 \ldots\ 2\ 1 \mid 24\ 13 \ldots\ 6\ 12 \mid 30\ 15\ 25 \mid 20\ 5\ 10 \mid 0 \mid 7\ 21\ 28\ 14.$$

Condition (iv) of Theorem 4.1 is restrictive, as $\mathbb{U}_n$ may well not contain any element $y$ such that $\mathbb{U}_n = \langle 2, y\rangle_n$. For example, each of the $n$-values 119 and 161 is such that $9 \in \langle 2\rangle_n$ and $\mathbb{U}_n = \langle 2\rangle_n \cup -\langle 2\rangle_n \cup 3\langle 2\rangle_n \cup -3\langle 2\rangle_n$. Thus, for each of 119 and 161, the set $\langle 2\rangle_n$ contains all the squares from $\mathbb{U}_n$, so that, for any element $y$, the set $\langle 2, y\rangle_n$ can contain no more than half of the elements from $\mathbb{U}_n$. The relevant properties of the integers 119 and 161 are that (i) neither of them has 2 as a primitive $\lambda$-root [9], and (ii) each is the product of distinct odd primes $p$ and $q$ neither of which has 2 as a primitive root. Our paper [5] failed to provide any terraces for such composite integers (but was working under the restriction—not operating in the present paper—that all terraces should have the minimum number of segments). We therefore now develop our present methodology to give a theorem for some of these integers, including the values 119 and 161 already mentioned. In this theorem, the pair of segments starting with the element $2^{-1}$ is obtained as in previous theorems, with $i = 1$ and $y = 3^{-1}$.

Table 4
Specimen parameter-sets for $\mathbb{Z}_n$ terraces available from Theorem 4.1, $n < 500$

| $n$ | $k$ | $\mathrm{ord}_n(2)$ | $p$ | $q$ | $\mathrm{ord}_p(2)$ | $\mathrm{ord}_q(2)$ | $i$ | $y$ | $x$ |
|---|---|---|---|---|---|---|---|---|---|
| 35 | 2 | 12 | 5 | 7 | 4 | 3 | 1 | 12 | 6 |
| 55 | 2 | 20 | 5 | 11 | 4 | 10 | 1* | 37 | 2 |
| 65 | 4 | 12 | 5 | 13 | 4 | 12 | 1* | 22 | 4 |
| 77 | 2 | 30 | 11 | 7 | 10 | 3 | 7 | 61 | 2 |
| 85 | 8 | 8 | 5 | 17 | 4 | 8 | 1 | 57 | 1 |
| 91 | 6 | 12 | 7 | 13 | 3 | 12 | 1 | 61 | 7 |
| 95 | 2 | 36 | 5 | 19 | 4 | 18 | 5 | 92 | 9 |
| 115 | 2 | 44 | 5 | 23 | 4 | 11 | 5 | 42 | 20 |
| 119† | 4 | 24 | – | – | – | – | – | – | – |
| 133 | 6 | 18 | 7 | 19 | 3 | 18 | 1 | 89 | 17 |
| 143 | 2 | 60 | 11 | 13 | 10 | 12 | 37 | 61 | 12 |
| | | | 13 | 11 | 12 | 10 | 41 | 136 | 5 |
| 145 | 4 | 28 | – | – | – | – | – | – | – |
| 155 | 6 | 20 | 5 | 31 | 4 | 5 | 1 | 52 | 23 |
| 161† | 4 | 33 | – | – | – | – | – | – | – |
| 185 | 4 | 36 | 5 | 37 | 4 | 36 | 1* | 62 | 28 |
| 187 | 4 | 40 | 11 | 17 | 10 | 8 | 33 | 91 | 5 |
| 203 | 2 | 84 | 29 | 7 | 28 | 3 | 13 | 159 | 2 |
| 205 | 8 | 20 | 5 | 41 | 4 | 20 | 1 | 137 | 21 |
| 209 | 2 | 90 | 11 | 19 | 10 | 18 | 67 | 61 | 15 |
| 215†† | 6 | 28 | – | – | – | – | – | – | – |
| 217 | 12 | 15 | – | – | – | – | – | – | – |
| 221 | 8 | 24 | – | – | – | – | – | – | – |
| 235 | 2 | 92 | 5 | 47 | 4 | 23 | 21 | 92 | 42 |
| 247 | 6 | 36 | – | – | – | – | – | – | – |
| 253 | 2 | 110 | 11 | 23 | 10 | 11 | 27 | 226 | 9 |
| 259 | 6 | 36 | 7 | 37 | 3 | 36 | 13 | 208 | 25 |
| 265 | 4 | 52 | 5 | 53 | 4 | 52 | 21 | 77 | 14 |
| 287† | 4 | 60 | – | – | – | – | – | – | – |
| 295 | 2 | 116 | 5 | 59 | 4 | 58 | 1* | 197 | 10 |
| 299 | 2 | 132 | 13 | 23 | 12 | 11 | 5 | 19 | 13 |
| 305 | 4 | 60 | 5 | 61 | 4 | 60 | 1* | 102 | 53 |
| 319 | 2 | 140 | 29 | 11 | 28 | 10 | 13 | 14 | 6 |
| 323 | 4 | 72 | – | – | – | – | – | – | – |
| 329† | 4 | 69 | – | – | – | – | – | – | – |
| 335 | 2 | 132 | 5 | 67 | 4 | 66 | 13 | 157 | 65 |
| 341 | 30 | 10 | – | – | – | – | – | – | – |
| 355 | 2 | 140 | 5 | 71 | 4 | 35 | 13 | 67 | 49 |
| 365# | 8 | 36 | – | – | – | – | – | – | – |
| 371 | 2 | 156 | 53 | 7 | 52 | 3 | 25 | 26 | 4 |
| 377 | 4 | 84 | 29 | 13 | 28 | 12 | 1 | 126 | 7 |
| 391 | 4 | 88 | – | – | – | – | – | – | – |
| 395 | 2 | 156 | 5 | 79 | 4 | 39 | 1 | 132 | 66 |
| 403 | 6 | 60 | – | – | – | – | – | – | – |
| 407 | 2 | 180 | 11 | 37 | 10 | 36 | 7 | 83 | 26 |
| 413 | 2 | 174 | 59 | 7 | 58 | 3 | 49 | 89 | 5 |
| 415 | 2 | 164 | 5 | 83 | 4 | 82 | 1 | 277 | 14 |
| 427 | 6 | 60 | 7 | 61 | 3 | 60 | 1 | 285 | 13 |
| 437 | 2 | 198 | – | – | – | – | – | – | – |
| 445 | 8 | 44 | 5 | 89 | 4 | 11 | 1 | 297 | 28 |
| 451 | 20 | 20 | – | – | – | – | – | – | – |
| 469 | 6 | 66 | 7 | 67 | 3 | 66 | 1 | 313 | 6 |
| 473 | 6 | 70 | – | – | – | – | – | – | – |
| 481 | 12 | 36 | – | – | – | – | – | – | – |
| 485 | 8 | 48 | 5 | 97 | 4 | 48 | 13 | 417 | 17 |
| 493 | 8 | 56 | – | – | – | – | – | – | – |
| 497† | 4 | 105 | – | – | – | – | – | – | – |

An asterisk * marks a case covered by Section 5.3 of [5]; a dagger † marks a case covered by Theorem 4.2; a double dagger †† marks a case covered by Theorem 4.3; a hash # marks a case covered by Theorem 4.4.

**Theorem 4.2.** *Let $n = 7q$ where $q$ is a prime, $q \equiv 17$ or $23 \pmod{24}$, such that $\mathrm{ord}_n(2) = 3(q-1)/2$. With $p = 7$, let* **P** *and* **Q** *be as defined in Theorem* 4.1. *Write $x = 3^{-1} \cdot 2^{-2}$. Then*

$$q\mathbf{P} \mid 0 \mid 7x\mathbf{Q}^{\mathrm{rev}} \mid 2^{-1}\ 2^{-2} \ldots\ 2^{1}\ 2^{0} \mid 3^{-1}\cdot 2^{1}\ 3^{-1}\cdot 2^{2} \ldots\ 3^{-1}\cdot 2^{0} \mid$$
$$-3^{-1}\cdot 2^{-1}\ -3^{-1}\cdot 2^{0} \ldots\ -3^{-1}\cdot 2^{-2} \mid -3^{-2}\cdot 2^{-1}\ -3^{-2}\cdot 2^{0} \ldots\ -3^{-2}\cdot 2^{-2}$$

*is a terrace for $\mathbb{Z}_n$.*

**Proof.** Since $\mathrm{ord}_{7q}(2) = \mathrm{lcm}(\mathrm{ord}_7(2), \mathrm{ord}_q(2)) = \mathrm{lcm}(3, \mathrm{ord}_q(2))$, we can have $\mathrm{ord}_n(2) = 3(q-1)/2$ iff $\mathrm{ord}_q(2) = (q-1)/2$ and $q \not\equiv 1 \pmod 3$. Thus 2 must be a square modulo $q$ with $q \equiv 5 \pmod 6$, so $q \equiv 17$ or $23 \pmod{24}$.

As 2 is a square both modulo 7 and modulo $q$ it is a square modulo $n$, and $3 \notin \langle 2\rangle_n$. Also, by Lemma 1.4, $-1 \notin \langle 2\rangle_n$. Suppose that $-3 \in \langle 2\rangle_n$. Then $-3$ is a square modulo $q$; but this requires $q \equiv 1 \pmod 6$, giving a contradiction. Thus $\langle 2\rangle_n$, $-\langle 2\rangle_n$, $3\langle 2\rangle_n$ and $-3\langle 2\rangle_n$ are all disjoint and their union is $\mathbb{U}_n$.

The missing differences and fence differences are easily checked. □

**Note 4.2.** In the range $2 < n < 1000$, this theorem covers $n = 119$, 161, 287, 329, 497 and 959.

**Example 4.2.** For $n = 119 = 7 \times 17$, the terraces obtainable from Theorem 4.2 include the following, where the first 3 segments constitute 17 times a terrace for $\mathbb{Z}_7$, and the three segments starting from the zero element constitute 7 times a terrace for $\mathbb{Z}_{17}$:

$$51\ 85\ 102 \mid 34\ 68\ 17 \mid 0 \mid 105\ 112\ 56\ 28\ 14\ 7\ 63\ 91 \mid 21\ 42\ 84\ 49\ 98\ 77\ 35\ 70 \mid$$
$$60\ 30 \ldots\ 2\ 1 \mid 80\ 41 \ldots\ 20\ 40 \mid 99\ 79 \ldots\ 114\ 109 \mid 33\ 66 \ldots\ 38\ 76.$$

The conditions in Theorem 4.2 include the requirements that

(i) $\mathbb{U}_n = \langle 2, 3\rangle_n \cup -\langle 2, 3\rangle_n$, and
(ii) $|\mathbb{U}_n| = 2|\langle 2, 3\rangle_n| = 4|\langle 2\rangle_n|$.

Now, to obtain Theorem 4.3, we develop the ideas just used to cover cases with the requirement (ii) replaced by

(ii′) $|\mathbb{U}_n| = 2|\langle 2, 3\rangle_n| = 6|\langle 2\rangle_n|$.

The final six segments of a terrace from Theorem 4.3 fall into two sets of three, the first set, starting with the element $2^{-1}$, again being obtained as previously, with $i = 1$ and $y = 3^{-1}$.

**Theorem 4.3.** *Let $n = 5q$ where $q$ is a prime, $q \equiv 19 \pmod{24}$, such that $\mathrm{ord}_n(2) = |\mathbb{U}_n|/6$ and $\mathbb{U}_n = \langle 2, 3\rangle_n \cup -\langle 2, 3\rangle_n$ where $3^3 \in \langle 2\rangle_n$ and $7 \in \langle 2, 3\rangle_n$. With $p = 5$, let* **P** *and* **Q** *be as defined in Theorem* 4.1. *Write $x = 3^{-2} \cdot 2^{-2}$ and $w = -7x$. Then*

$$q\mathbf{P} \mid 0 \mid 25x\mathbf{Q}^{\mathrm{rev}} \mid 2^{-1}\ 2^{-2} \ldots\ 2^{0} \mid 3^{-1}\cdot 2^{1}\ \ 3^{-1}\cdot 2^{2} \ldots\ 3^{-1}\cdot 2^{0} \mid$$
$$3^{-2}\cdot 2^{1}\ \ 3^{-2}\cdot 2^{2} \ldots\ 3^{-2}\cdot 2^{0} \mid 2^{1}w\ 2^{2}w \ldots\ 2^{0}w \mid$$
$$3^{-1}\cdot 2^{1}w\ \ 3^{-1}\cdot 2^{2}w \ldots\ 3^{-1}\cdot 2^{0}w \mid 3^{-2}\cdot 2^{1}w\ \ 3^{-2}\cdot 2^{2}w \ldots\ 3^{-2}\cdot 2^{0}w$$

*is a terrace for $\mathbb{Z}_n$.*

**Proof.** The checking of the missing and fence differences is straightforward; the choice of $w$ ensures that $2w - 3^{-2} = (n-1)/2$. The reason for the requirement $q \equiv 19 \pmod{24}$ is as follows. The condition $\mathrm{ord}_n(2) = 4(q-1)/6$ requires either $\mathrm{ord}_q(2) = (q-1)/6$, an odd number, or $\mathrm{ord}_q(2) = (q-1)/3$ and $q - 1 \equiv 2 \pmod 4$; in both cases we require $q \equiv 7 \pmod{12}$. So $q \equiv 7$ or $19 \pmod{24}$. But if $q \equiv 7 \pmod{24}$, then 2 is a square and 3 a nonsquare modulo $q$, so that $3^3 \in \langle 2\rangle_n$ is impossible. So $q \equiv 19 \pmod{24}$. □

**Note 4.3.** In the range $2 < n < 1000$, Theorem 4.3 covers only $(n, q) = (215, 43)$, for which $7 \in 3^2\langle 2\rangle_n$.

**Example 4.3.** For $(n, q) = (215, 43)$ we can use Theorem 4.3 with the values $x = 6$ and $w = -42 = 173$ to obtain $\mathbb{Z}_{215}$ terraces of the form

$$43\mathbf{P} \mid 0 \mid 150\mathbf{Q}^{\text{rev}} \mid$$
$$108\ \ 54 \ldots\ \ 2\ \ 1 \mid 144\ \ 73 \ldots\ \ 36\ \ 72 \mid 48\ \ 96 \ldots\ \ 12\ \ 24 \mid$$
$$131\ \ 47 \ldots\ \ 194\ \ 173 \mid 187\ \ 159 \ldots\ \ 208\ \ 201 \mid 134\ \ 53 \ldots\ \ 141\ \ 67.$$

Finally, to provide neat coverage of $n = 365$, we give a related theorem where the requirement $\mathbb{U}_n = \langle 2, 3\rangle_n \cup -\langle 2, 3\rangle_n$ has been replaced by an *ad hoc* condition.

**Theorem 4.4.** *Let $n = 5q$ where $q$ is a prime, $q \equiv 1 \pmod 8$, such that $\text{ord}_n(2) = |\mathbb{U}_n|/8$ and $|\langle 2, 3\rangle_n| = |\mathbb{U}_n|/2$. Suppose that $\mathbb{U}_n = \langle 2, 3\rangle_n \cup 29\langle 2, 3\rangle_n$. Write $v = 29 \cdot 3^{-3}$ and $x = -3^{-3} \cdot 2^{-1} v$. Write $\mathbf{R}$ for the sequence of segments*

$$2^{-1}\ \ 2^{-2} \ldots\ \ 2^0 \mid 3^{-1} \cdot 2^1\ \ \ 3^{-1} \cdot 2^2 \ldots\ \ 3^{-1} \cdot 2^0 \mid$$
$$3^{-2} \cdot 2^1\ \ \ 3^{-2} \cdot 2^2 \ldots\ \ 3^{-2} \cdot 2^0 \mid 3^{-3} \cdot 2^1\ \ \ 3^{-3} \cdot 2^2 \ldots\ \ 3^{-3} \cdot 2^0$$

*With $p = 5$, let $\mathbf{P}$ and $\mathbf{Q}$ be defined as in Theorem* 4.1. *Then*

$$\mathbf{R} \mid v\mathbf{R} \mid 25x\mathbf{Q} \mid 0 \mid q\mathbf{P}^{\text{rev}}$$

*is a terrace for $\mathbb{Z}_n$.*

**Proof.** The checking of the differences is routine. □

**Example 4.4.** For $(n, q) = (365, 73)$ we can use Theorem 4.4 with $v = 312$ and $x = 197$ to obtain terraces for $\mathbb{Z}_{365}$.

**Note 4.4.** In the range $2 < n < 1000$, Theorem 4.4 covers only $(n, q) = (365, 73)$ and $(965, 193)$. For these two cases, $\text{ord}_q(2) = (q - 1)/8$ and $(q - 1)/2$, respectively.

## Acknowledgement

We are grateful to Dr Wilson Stothers (University of Glasgow) for informing us of Theorem 1.2.

## References

[1] I. Anderson, D.A. Preece, Locally balanced change-over designs, Utilitas Math. 62 (2002) 33–59.
[2] I. Anderson, D.A. Preece, Power-sequence terraces for $\mathbb{Z}_n$ where $n$ is an odd prime power, Discrete Math. 261 (2003) 31–58.
[3] I. Anderson, D.A. Preece, Some narcissistic half-and-half power-sequence $\mathbb{Z}_n$ terraces with segments of different lengths, Cong. Numer. 163 (2003) 5–26.
[4] I. Anderson, D.A. Preece, Narcissistic half-and-half power-sequence terraces for $\mathbb{Z}_n$ with $n = pq^t$, Discrete Math. 279 (2004) 33–60.
[5] I. Anderson, D.A. Preece, Some power-sequence terraces for $\mathbb{Z}_{pq}$ with as few segments as possible, Discrete Math. 293 (2005) 29–59.
[6] I. Anderson, D.A. Preece, Some $\mathbb{Z}_{n-1}$ terraces from $\mathbb{Z}_n$ power-sequences, $n$ being an odd prime power, Proc. Edin. Math. Soc. 50 (2007), to appear.
[7] R.A. Bailey, Quasi-complete Latin squares: construction and randomisation, J. Roy. Statist. Soc. Ser. B 46 (1984) 323–334.
[8] N.G.W.H. Beeger, On a new case of the congruence $2^{p-1} = 1\ (p^2)$, Messenger Math. 51 (1922) 149–150.
[9] P.J. Cameron, D.A. Preece, Notes on Primitive $\lambda$-roots, ⟨http://www.maths.qmul.ac.uk/∼pjc/csgnotes/lambda.pdf⟩.
[10] W.J. LeVeque, Topics in Number Theory, vol. 1, Addison-Wesley, Reading, MA, 1956.
[11] W. Meissner, Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$, Akad. d. Wiss., Berlin, Sitzungsb. 35 (1913) 663–667.
[12] A. Wieferich, Zum letzten Fermatschen Theorem, J. Reine Angew. Math. 136 (1909) 293–302.